CLAIMS

What is claimed is:

1. A method for determining online financial transaction veracity, the method comprising:

a) determining a network address associated with an online payer in connection with an online payment instruction;

b) determining an online payer location associated with said network address;

c) receiving a payment instrument identification from said online payer;

d) comparing said online payer location to a valid payment location profile associated with said payment instrument identification; and

e) identifying said online payment instruction as a suspected fraudulent online payment attempt where said online payer location does not match said valid payment location profile.

2. A method according to claim 1 wherein said identifying step e) comprises authorizing said online payment instruction as being valid where said online payer location matches said valid payment location profile.

3. A method according to claim 1 wherein said identifying step e) comprises rejecting said online payment instruction where said online payer location does not match said valid payment location profile.

4. A method according to claim 1 and further comprising providing said suspected fraudulent online payment attempt to a payee to determine whether said payment attempt is fraudulent.

5. A method according to claim 1 wherein said determining step a) comprises determining said network address of a communications device through which said online payer makes said online payment instruction.

6. A method according to claim 5 wherein said determining step a) comprises determining an IP address of said communications device.

7. A method according to claim 1 wherein said determining step b) comprises representing said online payer location as a geographical location.

8. A method according to claim 7 wherein said determining step b) comprises representing said online payer location as a country.

9. A method according to claim 7 wherein said determining step b) comprises representing said online payer location as a city.

10. A method according to claim 6 wherein said determining step b) comprises representing said online payer location as an IP subnet address.

11. A method according to claim 1 wherein said receiving step c) comprises receiving a credit card identification code.

12. A method according to claim 1 wherein said receiving step c) comprises receiving a debit card identification code.

13. A method according to claim 1 and further comprising:

comparing the time at which said online payment instruction was made transaction takes place with the current time at either of said online payer location and a location indicated by said valid payment location profile; and

identifying said online payment instruction as a suspected fraudulent online payment attempt where said times do not match.

14. A method according to claim 1 and further comprising:

determining the language of a browser used to send said online payment instruction;

comparing said language with valid languages associated with the location of said online payer; and

identifying said online payment instruction as a suspected fraudulent online payment attempt where said browser language does not match any of said valid languages.

15. A method according to claim 1 and further comprising:

storing on a computer used to send said online payment instruction an identification identifying either of said computer and said online payer and indicating said suspected fraudulent online payment attempt;

retrieving said identification from said computer in conjunction with a subsequent online payment instruction; and

identifying said subsequent online payment instruction as a subsequent suspected fraudulent online payment attempt where said identification retrieved from said computer indicates said first-mentioned suspected fraudulent online payment attempt.

16. A method according to claim 1 and further comprising:

storing on a computer used to send said online payment instruction an identification identifying either of said computer and said online payer;

storing said identification and an indication of said suspected fraudulent online payment attempt in a database;

retrieving said identification from said computer in conjunction with a subsequent online payment instruction; and

identifying said subsequent online payment instruction as a subsequent suspected fraudulent online payment attempt where said identification retrieved from said computer matches said identification stored in said database.

17. A method for determining online financial transaction veracity, the method comprising:

comparing an element of an online payment instruction with a suspect payment instrucion profile; and

identifying said online payment instruction as a suspected fraudulent online payment attempt where said element matches said suspect payment instrucion profile.

18. A method according to claim 17 and further comprising:

determining a network address associated with said online payer in connection with said online payment instruction, and wherein said element is at least a portion of said network address.

19. A method according to claim 17 wherein said element is an e-mail address of an online payer.

20. A system for determining online financial transaction veracity, the system comprising:

means for determining a network address associated with an online payer in connection with an online payment instruction;

means for determining an online payer location associated with said network address;

means for receiving a payment instrument identification from said online payer;

means for comparing said online payer location to a valid payment location profile associated with said payment instrument identification; and

means for identifying said online payment instruction as a suspected fraudulent online payment attempt where said online payer location does not match said valid payment location profile.

21. A system according to claim 20 wherein said identifying means is operative to authorize said online payment instruction as being valid where said online payer location matches said valid payment location profile.

22. A system according to claim 20 wherein said identifying means is operative to reject said online payment instruction where said online payer location does not match said valid payment location profile.

23. A system according to claim 20 and further comprising means for providing said suspected fraudulent online payment attempt to a payee to determine whether said payment attempt is fraudulent.

24. A system according to claim 20 wherein said means for determining a network address is operative to determine said network address of a communications device through which said online payer makes said online payment instruction.

25. A system according to claim 24 wherein said means for determining a network address is operative to determine an IP address of said communications device.

26. A system according to claim 20 wherein said means for determining an online payer location is operative to represent said online payer location as a geographical location.

27. A system according to claim 26 wherein said means for determining an online payer location is operative to represent said online payer location as a country.

28. A system according to claim 26 wherein said means for determining an online payer location is operative to represent said online payer location as a city.

29. A system according to claim 25 wherein said means for determining an online payer location is operative to represent said online payer location as an IP subnet address.

30. A system according to claim 20 wherein said means for receiving is operative to receive a credit card identification code.

31. A system according to claim 20 wherein said means for receiving is operative to receive a debit card identification code.

32. A system according to claim 20 and further comprising:

means for comparing the time at which said online payment instruction was made transaction takes place with the current time at either of said online payer location and a location indicated by said valid payment location profile; and

means for identifying said online payment instruction as a suspected fraudulent online payment attempt where said times do not match.

33. A system according to claim 20 and further comprising:

means for determining the language of a browser used to send said online payment instruction;

means for comparing said language with valid languages associated with the location of said online payer; and

means for identifying said online payment instruction as a suspected fraudulent online payment attempt where said browser language does not match any of said valid languages.

34. A system according to claim 20 and further comprising:

means for storing on a computer used to send said online payment instruction an identification identifying either of said computer and said online payer and indicating said suspected fraudulent online payment attempt;

means for retrieving said identification from said computer in conjunction with a subsequent online payment instruction; and

means for identifying said subsequent online payment instruction as a suspected subsequent fraudulent online payment attempt where said identification retrieved from said computer indicates said first-mentioned suspected fraudulent online payment attempt.

35. A system according to claim 20 and further comprising:

means for storing on a computer used to send said online payment instruction an identification identifying either of said computer and said online payer;

means for storing said identification and an indication of said suspected fraudulent online payment attempt in a database;

means for retrieving said identification from said computer in conjunction with a subsequent online payment instruction; and

means for identifying said subsequent online payment instruction as a suspected subsequent fraudulent online payment attempt where said identification retrieved from said computer matches said identification stored in said database.

36. A system for determining online financial transaction veracity, the system comprising:

means for comparing an element of an online payment instruction with a suspect payment instrucion profile; and

means for identifying said online payment instruction as a suspected fraudulent online payment attempt where said element matches said suspect payment instrucion profile.

37. A system according to claim 36 and further comprising:

means for determining a network address associated with said online payer in connection with said online payment instruction, and wherein said element is at least a portion of said network address.

38. A system according to claim 36 wherein said element is an e-mail address of an online payer.